



PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G06F 1/00		A2	(11) International Publication Number: WO 00/31608
			(43) International Publication Date: 2 June 2000 (02.06.00)
(21) International Application Number: PCT/SE99/02115 (22) International Filing Date: 18 November 1999 (18.11.99) (30) Priority Data: 60/109,691 24 November 1998 (24.11.98) US 09/325,349 4 June 1999 (04.06.99) US (71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE). (72) Inventors: TUNELD, Mats; Östratonsvägen 29, S-224 68 Lund (SE). HOLOSHKA, David; Skolgatan 13, S-223 61 Lund (SE). (74) Agent: ERICSSON MOBILE COMMUNICATIONS AB; IPR Dept., S-221 83 LUND (SE).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>Without international search report and to be republished upon receipt of that report.</i>	
(54) Title: MOBILE TELEPHONE AUTO PC LOGON			
(57) Abstract The present invention is concerned with systems and methods for using a mobile telephone to automatically log a computer user onto a computer system. A subscriber identification module (SIM) is introduced to the computer system so that the computer system associates the SIM with the computer user. The SIM is then inserted into the mobile telephone. When the mobile telephone is powered on the user is prompted for a personal identification number (PIN). When the user wishes to log onto the computer system, the user establishes a communication channel between the mobile telephone and the computer. The mobile telephone and computer exchange identification information and the computer user is automatically logged onto the computer system.			

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

-1-

MOBILE TELEPHONE AUTO PC LOGON**RELATED APPLICATIONS**

5 This application is related to, and claims priority from U.S. Provisional Patent Application Serial No. 60/109,691, entitled "Mobile Phone Auto PC Logon", filed on November 24, 1998, the disclosure of which is incorporated here by reference.

BACKGROUND

10 The Global System for Mobile communication (GSM) describes a European standard for radiocommunication utilized by the corresponding Public Land Mobile Networks (PLMNs) in the region and in many other countries, which standard is intended to provide uniformity so that users can access radiocommunication systems throughout Europe and many other countries with minimal equipment compatibility problems.

15 In order for mobile telephones to operate in cellular telephone systems, the user of the mobile telephone must have a subscription with a network provider. In GSM systems, the mobile telephone is identified as having a subscription with a network provider through the use of a subscriber identity module (SIM). The SIM is a "smart card" comprising a processor and a memory. The SIM is designed
20 such that it may be removed from one mobile telephone and inserted into another mobile telephone with which the user wishes to use her subscription. In GSM the SIM is used to protect the mobile network against fraudulent access and to ensure subscriber privacy. This is accomplished through authentication of the subscriber to prevent access of unregistered users, radio path ciphering, in particular
25 ciphering of all subscriber information to prevent third party tapping, and subscriber identity protection to prevent subscriber location disclosure.

-2-

In order to protect information stored on computers, authentication mechanisms are used to verify that a user of a computer is an authorized user. Typical computer authentication mechanisms include a logon identification and a password. One way to increase the security of a computer system or network is to increase the number of characters in logon identifications and passwords. Further, some computer systems and networks require that the logon identification and password are changed on a regular basis, e.g., every three months. Computer users find it difficult to memorize long authentication codes every few months. Accordingly, what is needed is a secure way for the user to authenticate a computer system without having to memorize a logon identification and password.

SUMMARY

These and other drawbacks and difficulties found in authentication systems, for example computer systems, are overcome according to the present invention. According to exemplary embodiments of the present invention, a SIM card contained in a mobile telephone is associated with a user's computer account using a secure technique which exchanges identification information between the computer and the SIM. When the mobile telephone is powered on, the user is required to enter a Personal Identification Number (PIN). When the user of a mobile telephone, who has entered the correct PIN comes into communication with a computer, the mobile telephone exchanges the identification information with the computer and, if the user is authorized, the user is automatically logged onto the computer. Accordingly, the user only needs to memorize a short PIN in order to perform the authentication needed to log onto a computer.

In accordance with various embodiment described herein, the communication link between the computer and the mobile telephone can comprise a short-range wireless radio communications link, an infrared wireless communication link, or a cable connecting the computer and the mobile telephone. Alternatively, the communications link can be established when the mobile

-3-

telephone is inserted into a telephone battery charger located in proximity to the computer.

Further, exemplary embodiments of the present invention provide a method of configuring the mobile telephone and the computer system so the computer system associates the user of the mobile telephone with a user name and password stored in the computer system.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing objects, features and advantages of the present invention will be more readily understood upon reading the following detailed description in conjunction with the drawings in which:

Figure 1 illustrates the authentication system according to an exemplary embodiment of the present invention;

Figure 2 illustrates an exemplary method for configuration of the mobile telephone and the computer system;

Figure 3 illustrates an exemplary database record for storage and retrieval of a SIM ID and public key associated with a particular subscriber;

Figure 4 illustrates a exemplary arrangement which allows a mobile telephone to logon to a computer system of the present invention; and

Figure 5 illustrates an exemplary method for logging on to a computer system using a mobile telephone.

DETAILED DESCRIPTION

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular circuits, circuit components, and techniques, in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced in other embodiments that depart from these

-4-

specific details. In other instances, detailed descriptions of well-known methods, devices, and circuits are omitted so as not to obscure the description of the present invention.

5 The exemplary embodiments provide illustrative examples relating to mobile telephones which operate according to the GSM standard. However, those skilled in the art will appreciate that the concepts disclosed herein are equally applicable to mobile telephones which operate according to other standards. Likewise, some of the exemplary embodiments provide illustrative examples relating SIM cards for providing subscriber identification information, however, 10 the techniques described herein are equally applicable to other methods of providing subscriber identification information in a mobile telephone.

Figure 1 illustrates an exemplary embodiment of the hardware which is used to implement the present invention. A user inserts SIM 120 into mobile telephone 110. SIM 120 provides information necessary for the mobile telephone 15 110 to operate in the mobile network. When the mobile telephone 110 is powered on, the user is prompted for a PIN which would allow the user to operate the telephone. If the PIN entered by the user matches the PIN stored in SIM 120, then the user is able to operate mobile telephone 110.

Computer 140 can be any type of computer such as a "Wintel" computer comprising an Intel processor and using a Microsoft Windows operating system. 20 However, one skilled in the art will recognize that the computer could also use processors made by any manufacturer, e.g., Cyrix or AMD, Motorola, and any type of operating system, e.g., Unix and Apple's Macintosh operating system. Typically, for a user to access the operating system and application files which are stored on computer 140, the user must be logged onto the computer 140. Typical 25 logon procedures include a graphical user interface form with blanks for a user to enter a logon identification and a password. Once a user has enter the correct logon identification and password the user will be logged onto the computer 140.

-5-

In order for a user to implement the present invention, the computer system and the mobile telephone can be configured such that the user account or identity of mobile telephone 110 is associated with a user account or identity of the computer 140 (or a computer network). More specifically, SIM 120 will be associated with the account of a user of computer 140. According to an exemplary embodiment of the present invention, computer 140 runs Windows NT and the SIM can run programs written in the Java programming language.

Figure 2 illustrates an exemplary method for configuration of the system. Accordingly, in step 205 the mobile telephone is set in a mode wherein information can be written into the SIM, e.g., the SAT configuration mode. According to an exemplary embodiment of the present invention, SIM 120 contains a SIM application toolkit (SAT). SAT is a development environment incorporated in the GSM standard for writing programs which run on SIMs. To install the program which generates the public and private keys onto SIM 120, SIM 120 is inserted into smart card reader/writer 150. One skilled in the art will recognize that smart card reader/writer is only needed to install the programs which run on SIM 120, e.g., the program which generates public and private keys. Accordingly, to automatically logon to a PC according to the present invention does not require each computer to have a smart card reader/writer. The mobile telephone can be set in the SAT configuration mode by selecting the configure SAT option from the menu of functions available on the mobile telephone and by entering the correct PIN, i.e., an administrative PIN used for configuration of the mobile telephone. Alternatively, the PIN used for setting the mobile telephone in the SAT configuration mode may be the same PIN used to activate the mobile telephone.

In step 210, the computer 140 generates a set of public and private keys. The public key is stored in an administrative database in computer 140, or in a computer network, in accordance with step 215. Figure 3 illustrates a purely exemplary database record for storage and retrieval of a SIM ID and public key

-6-

associated with a particular user. In step 220, the private key is stored on the SIM 120. In addition the various parameters for coding data transferred between the mobile telephone 110 and the computer 140, are stored on the SIM 120, in accordance with step 225. The various parameters are the numbers used in the
5 RSA algorithm, e.g., two prime numbers.

Once the system has been configured to associate the SIM with one or more user accounts/identities of the computer system and the user of mobile telephone 110 has entered the PIN into the mobile telephone 110, the user may automatically log onto computer 140. Accordingly, the user will engage a communications link
10 between mobile telephone 110 and computer 140 to transfer authentication/identity information there between. According to an exemplary embodiment, the communication link between mobile telephone 110 and computer 140 is established via short range radio communications technology such as "Bluetooth" which is described in "Bluetooth--The Universal Radio Interface for Ad Hoc, Wireless
15 Connectivity" by Jaap Haartsen, Ericsson Review, No. 3, 1998, which is herein incorporated by reference. Of course those skilled in the art will appreciate that any other type of communication link can be employed. According to the exemplary embodiment using "Bluetooth", the user need only enter an area within the radio range of the computer for a communications link to be engaged between
20 the mobile telephone and the computer. According to this embodiment, computer 140, has a communication unit 130 attached to it, in order to communicate via the short range radio communications.

Figure 4 illustrates an exemplary arrangement which allows a mobile telephone user to logon to a computer system according to the present invention.
25 Computer 405 is running an operating system 450, wherein one of the components of the operating system is resource manager 410. A smart card device driver 415 interfaces between the operating system 450 running on computer 405, and SIM 430, as illustrated in figure 4. In an exemplary embodiment, computer 140 is running an operating system which uses Microsoft Smart Card Technology.

-7-

Microsoft Smart Card Technology is currently available for the following operating systems, Microsoft Windows 95, Windows 98, NT 4 and NT 5.

Additionally, future versions of Microsoft operating systems are expected to support the Smart Card Technology. Smart Card Technology uses a resource

5 manager to manage and control all applications access to the smart card.

Microsoft Smart Card Technology is described in "Smart Cards White Paper", Microsoft Corporation, April 24, 1998, which is herein incorporated by reference.

Although an exemplary embodiment of the present invention is described herein with reference to the Windows NT operating system, one skilled in the art will

10 recognize that the present invention can be implemented using any type of operating system which has the ability, or can be modified, to communicate with smart cards. Device driver 415 and resource manager 410 are components of the

Smart Card Technology. Accordingly, one skilled in the art will recognize that in other operating system environments, the operating system components responsible

15 for logon will perform functions similar to those described herein with regard to the device driver 415 and the resource manager 410. Device driver 415

communicates with mobile telephone 425 through communications link 420.

Identification and authentication information are exchanged between SIM 430, via mobile telephone 425, and the computer 405, via device driver 415. Accordingly,

20 device driver 415 translates information received from mobile telephone 425 into a form which is compatible with resource manager 410, and also translates data from resource manager 410 into a form which mobile telephone 425 can convey to SIM 430.

25 An exemplary method for logging onto a computer system using a SIM in a mobile telephone is illustrated in Figure 5. In step 510, one of the computer and the activated mobile telephone recognize a proximity to the other. According to one exemplary embodiment this is accomplished by the computer detecting a short range signal emitted by the mobile telephone. Alternatively, the mobile telephone can detect a short range signal emitted by the computer. In step 515, the computer

-8-

determines whether a mobile telephone has been found. If the computer does not find a mobile telephone, in accordance with the "NO" path out of decision step 515, then the computer returns to step 510 to search for a mobile telephone. If a mobile telephone is found by the computer, in accordance with the "YES" path out of decision step 515, then components of the smart card technology on the Windows NT computer sends an instruction to the mobile telephone to activate the authentication application in the SIM, in accordance with step 520.

In step 525, the computer queries the mobile telephone using an AT command to determine whether the detected mobile telephone has the capability of generating a digital signature and whether such capability has been activated in the mobile telephone. AT stands for attention, and AT commands are standard commands used for serial communication with computers. The digital signature is a string of bits which is produced by the RSA algorithm using the private key and a random string of bits. The digital signature is used to uniquely, and securely, identify the mobile telephone. According to an exemplary embodiment of the present invention, the mobile telephone will have an option on one of its menus to activate and deactivate the sending of a digital signature. If the digital signature capability is not activated, in accordance with the "NO" path out of decision step 525, then the system returns to step 510 and the computer continues to search for mobile telephones.

If the digital signature capability has been activated by the mobile telephone, in accordance with the "YES" path out of decision step 525, then the smart card driver 415 sends an AT command to the mobile telephone requesting the SIM ID number, in accordance with step 530. After the SIM ID is returned from the mobile telephone to the computer, the smart card driver 415 notifies the resource manager 410 that a SIM card is inserted in the mobile telephone. The resource manager 410 notifies a graphical identification and authentication dynamic-link library (GINA) that a card is inserted, in accordance with step 550.

-9-

GINA allows developers to implement smart-card authentication mechanisms in place of the standard Windows NT user name and password authentication.

In step 560, GINA retrieves the authentication information from the SIM. Step 560 involves GINA calling the Crypto applications program interface (CryptoAPI), which results in data transfer between the card and the smart card driver. This data transfer involves the smart card driver sending (via a transceiver device connected to computer 405), a random pattern of bits to the SIM. This information can, for example, be stored in the SMS (short message service) memory of the mobile telephone. The SIM card in the mobile telephone encodes the random data using the RSA algorithm and with the private key. The coded data, i.e., the digital signature, is sent back to the smart card driver. The encrypted random bits are decrypted by either the smart card driver or the CryptoAPI service provider using the SIM's public key. The decrypted random bits are compared to the transmitted random bits, in accordance with step 570. If the data matches then the user is logged onto the computer in accordance with step 580. The logon procedure of step 580 is completed by GINA in cooperation with other components of the authentication system, e.g., LAN Security Architecture (LSA), Kerberos, Key Distribution Center (KDC).

Although the description above describes logging onto a computer, one skilled in the art will recognize that the invention is equally applicable to logging onto computer networks or any device which requires authentication. Further, although communications unit 130 is shown as a separate peripheral from computer 140, one of ordinary skill in the art will recognize that communications unit 130 can be incorporated in a PC card design and mounted inside of computer 140. In addition, although the exemplary embodiments describe the use of a PIN to activate the mobile telephone, the mobile telephone can also be activated by conventional voice activation systems.

Although the exemplary embodiment is discussed wherein the communications link between computer 140 and mobile telephone 110 is a radio

-10-

communications link, the present invention can be practiced with any type of communications link between the computer and mobile telephone. Accordingly, the communications link may be a cable attached between the two devices, e.g., an RS-232 cable. Alternatively, the communications link may be an IrDA link, i.e., an infrared link whose standards are defined by the Infrared Data Association. According to an exemplary embodiment, the authentication could be performed when the mobile telephone 110 is inserted into a cradle which recharges the mobile telephone's battery. In addition to being connected to a power source, the cradle is connected to the computer through any of the various communications links described herein. Additionally, when a user of the mobile telephone, who has already logged onto a computer, moves out of range of the computer, the user may be automatically logged off of the computer. Alternatively, when the mobile telephone moves out of range a password protected screen saver could be initiated to protect the computer users data.

While the present invention has been described using the forgoing exemplary embodiments, these embodiments are intended to be illustrative in all respects, rather than restrictive of the present invention. Thus, the scope of the present invention is instead set forth by the appended claims and encompasses any and all equivalents and modifications embraced thereby.

-11-

WHAT IS CLAIMED IS:

1. A method for logging onto a computer comprising the steps of:
establishing a communications channel between a mobile telephone and the
5 computer;
exchanging identification information between the mobile telephone and the
computer; and
logging a user of said mobile telephone onto the computer when the
identification information is verified by the computer.
10
2. A method in accordance with claim 1, further comprising the steps of:
entering a personal identification number when the mobile telephone is
powered on; and
activating the mobile telephone if the entered personal identification number
15 matches a personal identification number stored on a subscriber identity module in
said mobile telephone.
3. A method in accordance with claim 1 comprising the step of
associating the mobile telephone with the user of the computer.
20
4. A method in accordance with claim 3, wherein said step of associating the
mobile telephone comprises the steps of:
setting the mobile telephone into a configuration mode;
generating public and private keys;
25 storing the public key in a database on said computer; and
storing the private key and coding data on a smart card in said mobile
telephone.

-12-

5. A method in accordance with claim 1, wherein said step of establishing a communications channel comprises the steps of:

searching for a mobile telephone; and

5 determining whether a digital signature capability is present in the mobile telephone and whether the digital signature capability has been activated in said mobile telephone.

6. A method in accordance with claim 1, wherein the step of exchanging identification information comprises the steps of:

10 retrieving an identification number associated with a smart card;

notifying the computer that the smart card is inserted in the mobile telephone; and

retrieving authentication information from said smart card.

15 7. A method in accordance with claim 1, wherein the communications channel is a radio communications link.

8. A method in accordance with claim 1, wherein the communications channel is an infrared link.

20

9. A method in accordance with claim 1, wherein the communications channel is a cable connecting the mobile telephone and the computer.

25 10. A method in accordance with claim 1, wherein said communications channel is established when the mobile telephone is inserted into a battery charger, and wherein said battery charger is connected to the computer via said communications channel.

-13-

11. A system for logging onto a computer comprising:
a mobile telephone; and
a communications link between said mobile telephone and said computer,
wherein a user of said mobile telephone is logged onto said computer through an
5 authentication procedure which is performed over said communications link.
12. A system according to claim 11, wherein said mobile telephone includes a
subscriber identity module (SIM).
- 10 13. A system according to claim 11, wherein said card is a smart card.
14. A system according to claim 11, wherein said communications link is a
radio communication link.
- 15 15. A system according to claim 11, wherein said communications link is a
cable connecting the mobile telephone and the computer.
16. A system according to claim 11, wherein the authentication procedure
involves the mobile telephone coding random bits transmitted from the computer, and
20 wherein the mobile telephone transmits the encoded random bits to the computer.
17. A system according to claim 16, wherein said mobile telephone codes the
random bits using a private key, and wherein the computer decodes said encoded
random bits using a public key.
- 25 18. A method for automatically logging a mobile telephone user onto a
computer network comprising the steps of:
searching for a mobile telephone from a computer connected to said computer
network;

-14-

determining, by said computer, whether the mobile telephone has been set in an automatic logon mode;

checking, by said computer, an identification number of the mobile telephone;

performing an authentication procedure between the mobile telephone and the
5 computer.

19. A method in accordance with claim 18, wherein the mobile telephone is set in an automatic logon mode if a digital signature capability is present and is activated in the mobile telephone.

10

20. A method in accordance with claim 18, wherein the identification number is a subscriber identification module number stored on a smart card in the mobile telephone.

15

21. A method in accordance with claim 18, wherein the step of checking an identification number of the mobile telephone comprises the step of:
retrieving the identification number using an AT command.

20

22. A method in accordance with claim 18, wherein the authentication procedure comprises the steps of:

notifying an operating system component which is responsible for logon that a card is inserted in the mobile telephone;

retrieving and analyzing authentication information from the card; and

logging the user onto the computer if the authentication information is valid.

25

23. A method in accordance with claim 22, wherein the step of retrieving and analyzing authentication information comprises the steps of:

sending a random string of bits to the mobile telephone;

-15-

encoding, in the mobile telephone, the random string of bits with a private key;
returning the encoded random string of bits to the computer; and
decoding, in the computer, the encoded string of bits using a public key.

5

24. A method in accordance with claim 23, wherein the authentication information is valid when the string of bits decoded by the public key matches the random string of bit sent to the mobile telephone.

10

25. A method in accordance with claim 18, wherein the computer and the mobile telephone exchange information through a wireless communication channel.

26. A method in accordance with claim 25, wherein the wireless communication channel is a short range radio frequency channel.

15

27. A method in accordance with claim 25, wherein the wireless communication channel is an infrared communications channel.

20

28. A method in accordance with claim 18, wherein the computer and the mobile telephone exchange information through a cable.

25

29. A method in accordance with claim 18, further comprising the step of: automatically logging the user off of the computer network when the mobile telephone is a predetermined distance from said computer, wherein the predetermined distance is a range of a radio signal produced by the computer.

30. A method in accordance with claim 18, further comprising the step of: initiating a password protected screen saver on the computer when the mobile

-16-

telephone is a predetermined distance from said computer, wherein the predetermined distance is a range of a radio signal produced by the computer.

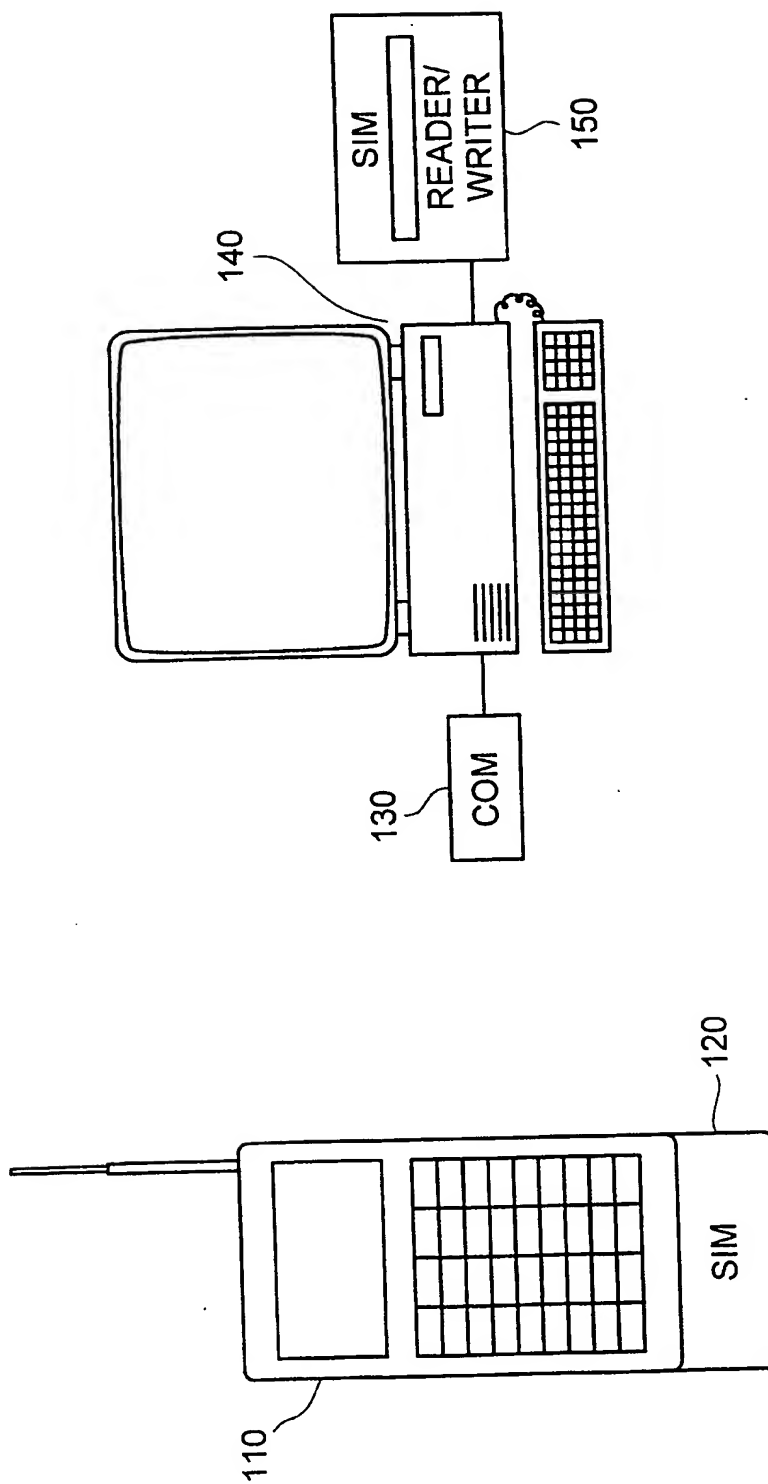


FIG. 1

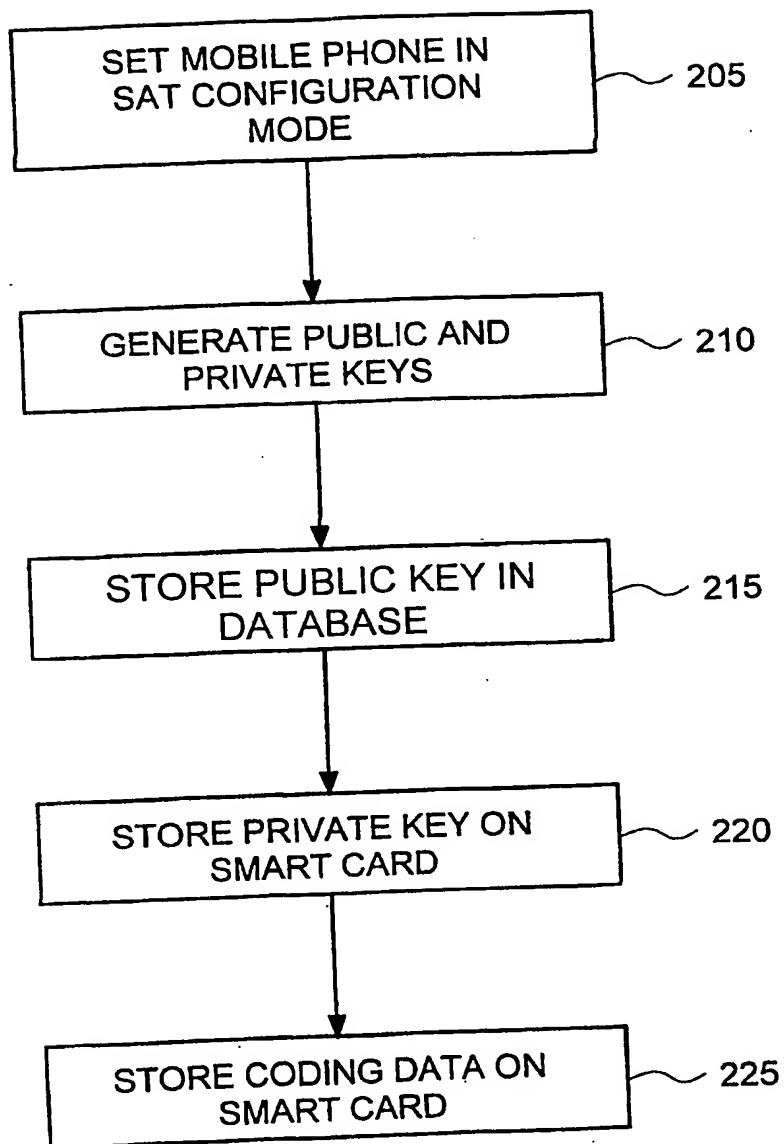


FIG. 2

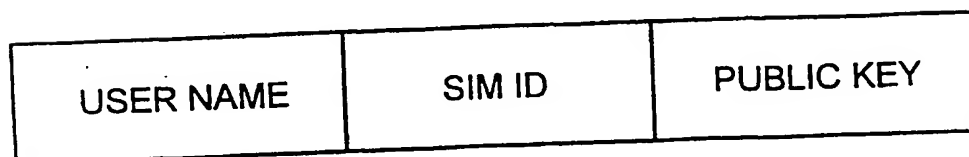


FIG. 3

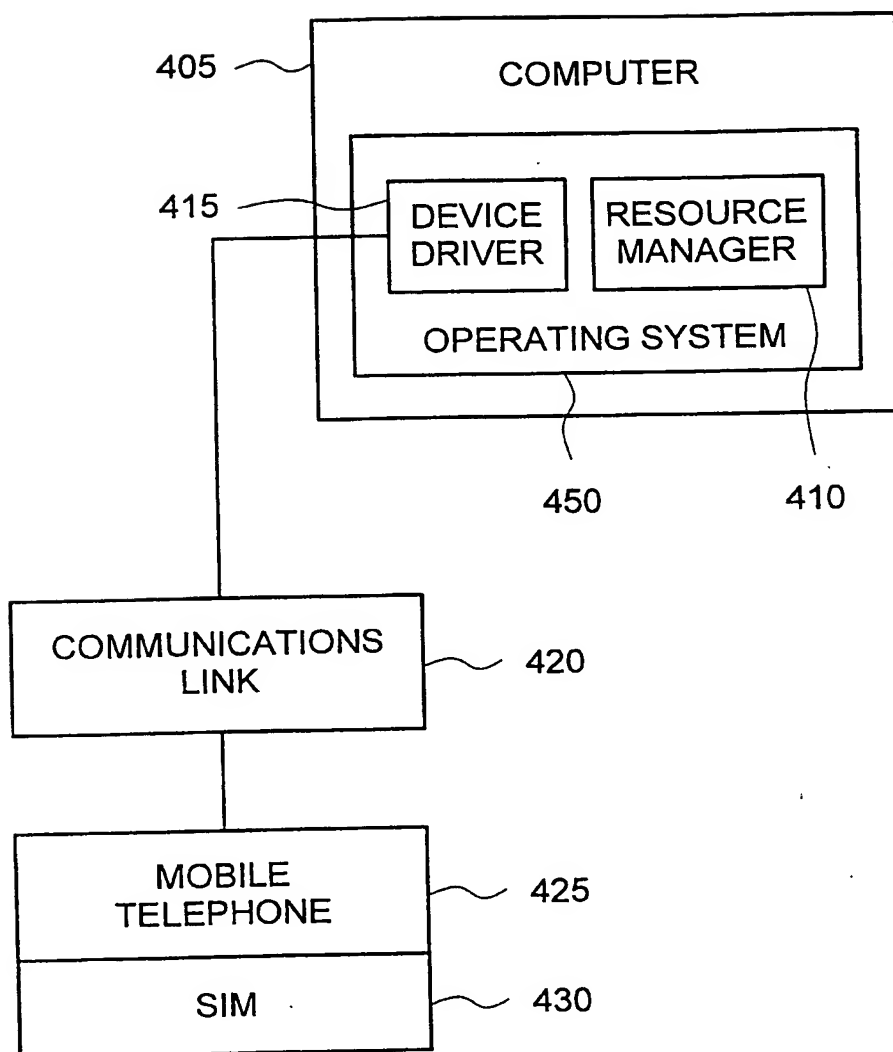


FIG. 4

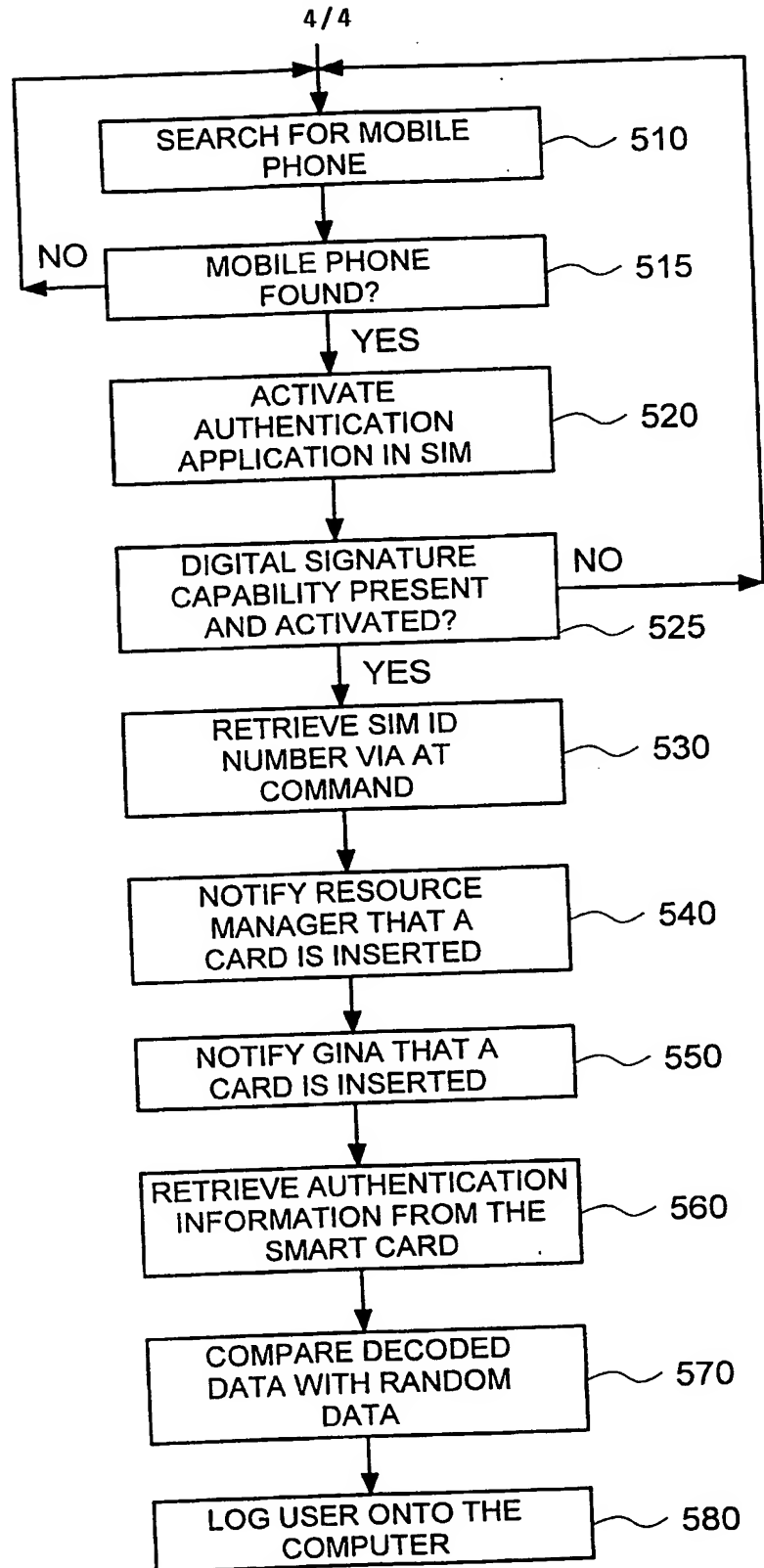


FIG. 5